**Swedish Certification Body for IT Security**

# Certification Report - OPPO Find X3 Pro on ColorOS 11.2

**Issue: 1.0, 2021-Oct-05**

*Authorisation: Helén Svensson, Lead certifier , CSEC*

Table of Contents

# 1 Executive Summary

The TOE is OPPO Find X3 Pro running on ColorOS 11.2. It is a personally-owned mobile phone for both personal and enterprise use. A detailed description of the TOE is provided in the table below:

| Device Name | Model Number | Chipset Vendor | CPU | OS Version | Build Number | Kernel Version |
|---|---|---|---|---|---|---|
| OPPO Find X3 Pro | CPH2173 | Qualcomm | Snapdragon 888 Octa-core | ColorOS 11.2 | CPH2173_11_A21 | Android version 11 kernel version 5.4 |

The TOE's physical boundary is the physical perimeter of its enclosure. The TOE runs ColorOS as its operating system on the Qualcomm Snapdragon 888 processor (refer to as Application Processor). The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behaviour. Further, the device provides support for downloadable MDM agents to be installed to limit or permit different functionality of the device. There is no built-in MDM agent pre-installed on the device.

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and through that connectivity interacts with MDM servers that allow administrative control of the TOE.

The ST claims exact conformance to Protection Profile for Mobile Device Fundamentals, Version 3.1 as of 2017-06-16.

The TOE is delivered to retailers and users can buy the TOE from them. [CCGUIDE] 1.3 "Security Acceptance of the TOE" describes that, when the user receives the phone, she needs to make sure that the package is intact and the seals are not broken or re-taped. And the user needs to check the ColorOS version and Android OS version in the "Settings" menu. How to update the software is also descried in the guidance.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden.

The evaluation was completed on 2021-09-27. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST), the Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017 (MDFPP31) and the Common Methodology for evaluation assurance level EAL1 augmented by ASE_SPD.1 and ALC_TSU_EXT.1.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

# 2 Identification

| Certification Identification | |
|---|---|
| Certification ID | CSEC2021001 |
| Name and version of the certified IT product | OPPO Find X3 Pro on ColorOS 11.2, Build Number CPH2173_11_A.21 |
| Security Target Identification | OPPO Find X3 Pro on ColorOS 11.2 Security Target, Guangdong OPPO Mobile Telecommunications Corp., Ltd, 2021-09-07, document version 1.1 |
| Protection Profile | Protection Profile for Mobile Device Fundamentals, NIAP, Version 3.1, 16 June 2017 |
| Assurance package | CCRA: PP compliant<br>SOGIS: EAL1 + ASE_SPD.1 and ALC_TSU_EXT.1 |
| Sponsor | Guangdong OPPO Mobile Telecommunications Corp., Ltd |
| Developer | Guangdong OPPO Mobile Telecommunications Corp., Ltd |
| ITSEF | atsec information security AB |
| Common Criteria version | 3.1 release 5 |
| CEM version | 3.1 release 5 |
| QMS version | 1.25 |
| Scheme Notes Release | 18.0 |
| Recognition Scope | CCRA, SOGIS, EA/MLA |
| Certification date | 2021-10-05 |

# 3 Security Policy

- Security Audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

## 3.1 Security audit

The TOE uses two forms of logs to record all the required management logging events specified in Table 1 of [MDFPPv3.1]:

- Security logs
- Logcat logs

Both logs are stored in memory and, when full, wrap around and overwrite the oldest records. The TOE protects both logs from unauthorized modification and deletion..

## 3.2 Cryptographic support

The TOE has two cryptographic modules:

- BoringSSL - the cryptographic algorithms provided by this module have been tested with the NIST ACVTS system.
- Hardware cryptographic module included in the Application Processor - the cryptographic algorithms provided by this module have NIST CAVP certificates.

Both cryptographic modules support random number generation, key generation/derivation, data encryption/decryption, hash, keyed hash, and digital signature.

## 3.3 User data protection

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, User data in files is protected using cryptographic functions, ensuring this data remains protected even if the device gets lost or is stolen. Data is protected such that only the app that owns the data can access it.

The TOE's evaluated configuration supports Android Enterprise profiles to provide additional separation between application and application data belonging to the Enterprise profile.

## 3.4 Identification and authentication

Except for answering calls, making emergency calls, using the cameras, using the flashlight, using the quick settings, and checking notifications, users need to authenticate using a passcode or a biometric (fingerprint).

The TOE enters a locked state after a (configurable) time of user inactivity, and the user is required to either enter his passcode or use biometric authentication (fingerprint) to unlock the TOE.

External entities connecting to the TOE via a secure protocol (Extensible Authentication Protocol Transport Layer Security (EAPTLS), Transport Layer Security (TLS)) can be authenticated using X.509 certificates.

## 3.5 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout [ST] as well as other functions commonly found in mobile devices. Some of the management functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled. Once the TOE has been enrolled and then un-enrolled, it will remove Enterprise applications and remove MDM policies.

## 3.6 Protection of the TSF

The TOE implements the following to protect the TSF and TSF data:

- Protection of cryptographic keys - keys are stored encrypted in Flash and plaintext key material cannot be exported.
- The TOE enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It also protects itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.
- Digital signature protection of the TSF image - all updates to the TSF need to be digitally signed.
- Software/firmware integrity self-test upon start-up - the TOE will not go operational when this test fails.
- Digital signature verification for apps.
- Access to defined TSF data and TSF services only when the TOE is unlocked.
- The TOE provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

## 3.7 TOE access

The TOE transitions to its locked state either immediately after a user initiates a lock by pressing the power button (if configured) or after a (also configurable) period of inactivity, and as part of that transition, the TOE will display a lock screen to obscure the previous contents and play a “lock sound” to indicate the phone’s transition; however, the TOE’S lock screen still displays email notifications, calendar appointments, user configured widgets, text message notifications, the time, date, call notifications, battery life, signal strength, and carrier network. But without authenticating first, a user cannot perform any related actions based upon these notifications.

## 3.8 Trusted path/channels

The TOE provides secured (encrypted and mutually authenticated) communication channels between itself and other trusted IT products through the use of IEEE 802.11-2012, 802.1X, EAP-TLS, TLS and HTTPS.

The TOE permits itself and applications to initiate communicate via the trusted channel, and the TOE initiates communications via the WPA2 (IEEE 802.11-2012, 802.1X with EAP-TLS) trusted channel for connection to a wireless access point. The TOE provides mobile applications and MDM agents access to HTTPS and TLS via published APIs, thus facilitating administrative communication and configured enterprise connections.

# 4 Assumptions and Clarification of Scope

## 4.1 Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.CONFIG (PP_MD_V3.1)

It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

A.NOTIFY (PP_MD_V3.1)

It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.

A.PRECAUTION (PP_MD_V3.1)

It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

## 4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.

T.EAVESDROP Network Eavesdropping (PP_MD_V3.1)

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.

T.NETWORK Network Attack (PP_MD_V3.1)

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software update of any applications or system software on the device. These attacks also include malicious web pages or email attachments which are usually delivered to devices over the network.

T.PHYSICAL Physical Access (PP_MD_V3.1)

An attacker, with physical access, may attempt to access user data on the Mobile Device including credentials. These physical access threats may involve attacks, which attempt to access the device through external hardware ports, impersonate the user authentication mechanisms, through its user interface, and also through direct and possibly destructive access to its storage media.

Note: Defending against device re-use after physical compromise is out of scope of this ST.

T.FLAWAPP Malicious or Flawed Application (PP_MD_V3.1)

Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally by its developer or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access.

They may also conduct attacks against the platform’s system software which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, cameras, and microphones) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

T.PERSISTENT Persistent Presence (PP_MD_V3.1)

Persistent presence on a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat in itself. In this case the device and its data may be controlled by an adversary at least as well as by its legitimate owner.

The Security Target contains no Organisational Security Policies (OSPs).

# 5 Architectural Information

The TOE OS manages the device hardware and provides the technologies with a rich API set required to implement native applications, it also provides the capability to approve or reject an application based upon the API access that the application requires (or to grant applications access at runtime).

The TOE provides a built-in Mobile Device Management (MDM) framework API, giving management features that may be utilized by external MDM solutions (not part of this evaluation), allowing enterprises to use profiles to control some of the device settings. Security management capabilities are also provided to users via the user interface of the device and to administrators through the installation of Configuration Profiles on the device by using MDM solutions.

The TOE provides cryptographic services for the encryption of data-at-rest within the TOE, for secure communication channels, for protection of Configuration Profiles, and for use by apps.

User data protection is provided by encrypting all of the user and mobile application data stored in the user's data partition, restricting access by apps and by restricting access until the user has been successfully authenticated.

User identification and authentication is provided by a user defined passphrase (and supplemented by biometric technologies) where the minimum length of the passphrase, passphrase rules, and the maximum number of consecutive failed authentication attempts can be configured by an administrator.

The TOE protects itself by having its own code and data protected from unauthorized access (using hardware provided memory protection features), by encrypting internal user and TOE Security Functionality (TSF) data using TSF protected keys and encryption/decryption functions, by self-tests, by ensuring the integrity and authenticity of TSF updates and downloaded apps, and by locking the TOE upon user request or after a defined time of user inactivity.

# 6 Documentation

OPPO Find X3 Pro on ColorOS 11.2 Administrator Guidance 1.1 [CC_GUIDE]

# 7 IT Product Testing

## 7.1 Evaluator Testing

The TOE was set up at the atsec office in Danderyd, Sweden and the testing was performed between April 2021 and June 2021. Re-testing was performed in September 2021.

The evaluator performed tests to ensure that the TOE behaves as specified in the ST and the guidance documentation as well as to perform tests described in [MDFPPv3.1].

Full testing was performed on OPPO Find X3 Pro Build Number CPH2173_11_A.18.

33 tests were re-executed on OPPO Find X3 Pro Build Number CPH2173_11_A.21.

All evaluator test cases were completed successfully

## 7.2 Penetration Testing

No potential vulnerabilities were found to be applicable to the TOE in its operational environment. The evaluator also performed multiple negative tests during independent testing without finding any issues. Thus the evaluator identified no need for penetration testing.

# 8 Evaluated Configuration

The TOE needs to be configured according to the instructions in [CCGUIDE] to be in a known state. More specifically, [CCGUIDE] 3.1 "Common Criteria Mode" describes how to configure the device into the Common Criteria mode, which includes the following settings:

- WiFi keys and Bluetooth keys are encrypted by default and can never be disabled
- Require a lockscreen password
- Disable Smart Lock and Face Authentication
- Disable Debugging Features (i.e. developer mode)
- Disable installation of applications from unknown sources
- Enable Audit Logging
- Disable USB Debugging

Besides, Bluetooth and Wi-Fi on the TOE should be configured according to the instructions in chapter 4 "Bluetooth Configuration" and chapter 5 "Wi-Fi Configuration" of [CCGUIDE], respectively.

# 9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC]. The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

| *Assurance Class / Family* | *Component* | *Verdict* |
|---|---|---|
| Security Target | ASE | |
| Conformance claims | ASE_CCL.1 | PASS |
| Extended components definition | ASE_ECD.1 | PASS |
| ST introduction | ASE_INT.1 | PASS |
| Security objectives for the operational environment | ASE_OBJ.1 | PASS |
| Stated security requirements | ASE_REQ.1 | PASS |
| Security Problem Definition | ASE_SPD.1 | PASS |
| TOE summary specification | ASE_TSS.1 | PASS |
| PP assurance activities | ASE_MDFPP.1 | PASS |
| Development | ADV | PASS |
| Basic functional specification | ADV_FSP.1 | PASS |
| Guidance documents | AGD | PASS |
| Operational user guidance | AGD_OPE.1 | PASS |
| Preparative procedures | AGD_PRE.1 | PASS |
| PP assurance activities | AGD_MDFPP.1 | PASS |
| Life-cycle support | ALC | PASS |
| Labelling of the TOE | ALC_CMC.1 | PASS |
| TOE CM coverage | ALC_CMS.1 | PASS |
| Timely Security Updates | ALC_TSU_EXT.1 | PASS |
| PP assurance activities | ALC_MDFPP.1 | PASS |
| Tests | ATE | PASS |
| Independent testing - conformance | ATE_IND.1 | PASS |
| PP assurance activities | ATE_MDFPP.1 | PASS |
| Vulnerability assessment | AVA | PASS |
| Vulnerability survey | AVA_VAN.1 | PASS |
| PP assurance activities | AVA_MDFPP.1 | PASS |

# 10 Evaluator Comments and Recommendations

None.

# 11 Bibliography


| | |
|---|---|
| ST | OPPO Find X3 Pro on ColorOS 11.2 Security Target, Guangdong OPPO Mobile Telecommunications Corp., Ltd, 2021-09-07, document version 1.1 |
| CC_GUIDE | OPPO Find X3 Pro on ColorOS 11.2 Administrator Guidance, Guangdong OPPO Mobile Telecommunications Corp., Ltd, 2021-09-07, document version 1.1 |
| MDFPPv3.1 | Protection Profile for Mobile Device Fundamentals, NIAP, Version 3.1, 16 June 2017 |
| CCpart1 | Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001 |
| CCpart2 | Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002 |
| CCpart3 | Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003 |
| CC | CCpart1 + CCpart2 + CCpart3 |
| CEM | Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004 |
| SP-002 | SP-002 Evaluation and Certification, CSEC, 2021-06-04, document version 33.0 |
| SP-188 | SP-188 Scheme Crypto Policy, CSEC, 2021-06-07, document version 11.0 |

# Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

## A.1 Scheme/Quality Management System

| Version | Introduced | Impact of changes |
|---|---|---|
| 1.25 | 2021-06-17 | None |
| 1.24.1 | Application | Original version |

## A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the ST
- Scheme Note 22 - Vulnerability Assessment
- Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs
- Scheme Note 25 Use of CAVP-tests in CC evaluations
- Scheme Note 27 - ST Requirements at the Time of Application for Certification
- Scheme Note 28 - Updated procedures for application, evaluation and certification
- Scheme Note 30 - CM of Third Party Components

The applicable versions are part of Scheme Note release 18.0